elastic security labs

2024

Elastic Global Threat Report 2023

Bedrohungstrends, die SOC-Führungskräfte kennen sollten

Der Elastic Global Threat Report 2024 wurde erstellt, um Sicherheitsteams und CISOs gleichermaßen verwertbare Einblicke zu geben. Er enthält die wichtigsten Erkenntnisse aus monatelangen Analysen von mehr als 1 Milliarde Datenpunkten, die sowohl aus öffentlichen als auch aus Elastic-spezifischen Telemetriedaten stammen. Diese Erkenntnisse wurden zu Einblicken aus den Daten und Handlungsempfehlungen für Ihr Unternehmen zusammengefasst.

Top Einblicke

01 Cloud-Umgebungen werden von Unternehmen falsch konfiguriert

In unserem neuen Abschnitt zum Cloud Security Posture Management (CSPM) wurden Umgebungen mit Benchmarks des Center for Internet Security (CIS) verglichen. Dabei stellte sich heraus, dass im Durchschnitt etwa 50 % der Umgebungen die Prüfungen nicht bestanden, unabhängig vom Cloud-Dienstanbieter (Cloud Service Provider, CSP).

02 Defense Evasion bleibt die am häufigsten verwendete Endpunkt-Taktik

Defense Evasion (Umgehung von Verteidigungsmaßnahmen) machte 38 % des Endpunktverhaltens aus, was darauf hindeutet, dass Angreifer mit Sicherheitssystemen umgehen können. Bemerkenswerterweise ist diese Zahl im Vergleich zum Vorjahr um 6 % gesunken, was zeigt, dass die Abwehrtools effektiv funktionieren.

03 Zugriffsberechtigungswarnungen nehmen weiter zu, insbesondere in der Cloud

Innerhalb von Cloud-Umgebungen entfielen 23 % der Aktivitäten auf den Bereich Credential Access. Darüber hinaus ist in Endpunktumgebungen im Jahresvergleich ein Anstieg dieser Techniken um 3 % zu verzeichnen. Dies ist auf die zunehmende Verbreitung von Informationsdieben und Vermittlern von Zugangsdaten sowie auf die Tatsache zurückzuführen, dass die Sicherheitstools immer besser sichtbar werden.

04 Gegner missbrauchen Defender-Tools, um effizient in Systeme einzudringen

53 % der beobachteten bösartigen Dateien wurden als offensive Sicherheitstools identifiziert – sie wurden von Unternehmen genutzt, um Schwachstellen zu entdecken, und von Angreifern missbraucht, um diese auszunutzen. Diese OSTs verfügen über große Forschungs- und Entwicklungsteams, um neue Funktionen wie Process Injection zu entwickeln: Dies ist eine Form der Defense Evasion, die in diesem Jahr für 53 % der Windows-Alarmereignisse verantwortlich war.

05 Generative KI hat weder die Anzahl noch die Auswirkungen der von uns beobachteten Angriffe erhöht.

Sicherheitsteams waren besorgt über einen bevorstehenden Ansturm von GenAI-Angriffen. Während wir einen leichten Anstieg des Bedrohungsvolumens beobachten konnten, hat GenAI die Technologien der Verteidiger mit Funktionen wie der Zusammenfassung von Alarmen und der Automatisierung von Aufgabenweitgehend gestärkt.

Wichtige Vorschläge

01 Überprüfen Sie Ihre Umgebung regelmäßig

Angreifer verlassen sich auf freizügige oder falsch konfigurierte Sicherheitskontrollen, um in Umgebungen einzudringen, und wenn sie erst einmal eingedrungen sind, konzentrieren sie sich auf die Manipulation von Sensoren und Daten. Benchmarking und Risikobewertungen können Ihnen dabei helfen, herauszufinden, ob Sie die besten Praktiken und Industriestandards nutzen, um den Zugang in Ihrem Unternehmen effektiv zu kontrollieren.

02 Bereiten Sie sich auf generative KI vor, indem Sie Ihre Sicherheitskontrollen optimieren

Die Zunahme von GenAI wird zu einem Anstieg von Social-Engineering-Versuchen führen. Während es immer eine gute Idee ist, Ihre Benutzer zu schulen, um diese und andere Versuche zu erkennen, sollten die Sicherheitsteams auch ihre Kontrollen und Berechtigungen überprüfen, um sicherzustellen, dass ein erfolgreicher Phishing-Versuch keinen langfristigen Schaden anrichtet.

03 Implementierung interaktiver Endpunkt-Agenten zur Neutralisierung von Defense-Evasion-Angriffen

Defense-Evasion-Angriffe sind seit ein paar Jahren die Haupttaktik. Auch wenn die Zahl der Angriffe abnimmt, nutzen Angreifer diese Methoden immer noch, um Umgebungen zu infiltrieren und in ihnen zu navigieren. Endpoint-Technologien wie Elastic Agent sorgen für Transparenz und Leistungsfähigkeit und reduzieren gleichzeitig die Anzahl der von Ihnen benötigten Tools.

04 Erstellen Sie einen robusten Reaktionsplan für offengelegte Anmeldeinformationen

Wir haben beobachtet, dass Techniken wie Brute Force und Zugriff auf Browser-Zugangsdaten aus einem verdächtigen Speicher regelmäßig eingesetzt werden. Die Rotation offengelegter Anmeldeinformationen und die Organisation schneller Workflows für die Reaktion auf Sicherheitsverletzungen werden einen großen Unterschied machen. Sicherheitsteams sollten eine Multi-Faktor-Authentifizierung vorschreiben, sofern dies nicht bereits geschehen ist.

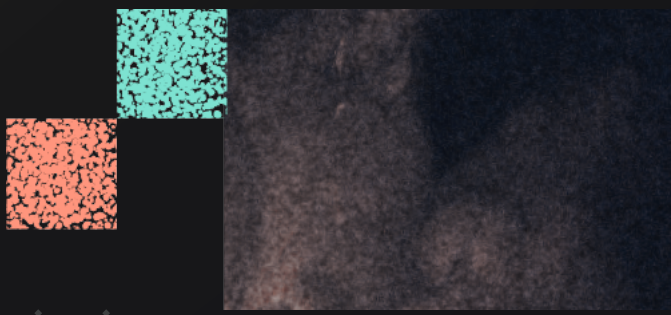
05 Vergleichen Sie Ihre Cloud-Umgebung mit den CIS-Benchmarks

Die CIS-Benchmarks sind ein Industriestandard und helfen Ihnen, schnell zu erkennen, welche Bereiche Aufmerksamkeit erfordern. Ihr Team sollte einen Plan zur Überwachung und Verbesserung Ihrer Punktzahl entwickeln, um die Erkennung von Bedrohungen zu verbessern und das Risiko langfristig zu verringern.

Bedrohungslandschaft beherrschen

Bereiten Sie sich auf die Entwicklung dieser und weiterer Bedrohungen vor. Alle unsere Vorschläge und eine vollständige Aufschlüsselung der aktuellen Bedrohungslandschaft finden Sie im Elastic Global Threat Report 2024. Sie können unseren Experten auch unter @ElasticSecLabs folgen.

Erfahren Sie, wie Elastic Security Ihre Sicherheitsabläufe modernisieren kann.



elastic security labs